



*April 2002*

---

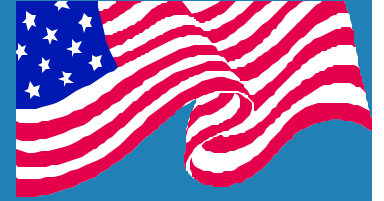
# Information Warfare and Cyber Defense

*Mr. Larry Wright  
Booz Allen Hamilton*

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 22-04-2002		2. REPORT TYPE Briefing		3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2002	
4. TITLE AND SUBTITLE Information Warfare and Cyber Defense Unclassified				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Wright, Larry ;				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS Booz Allen Hamilton 8283 Greensboro Drive McLean, VA22102				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS Booz Allen Hamilton ,				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE ,					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT See report.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 46	19. NAME OF RESPONSIBLE PERSON email from Booz Allen (IATAC), (blank) lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007		
					Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18

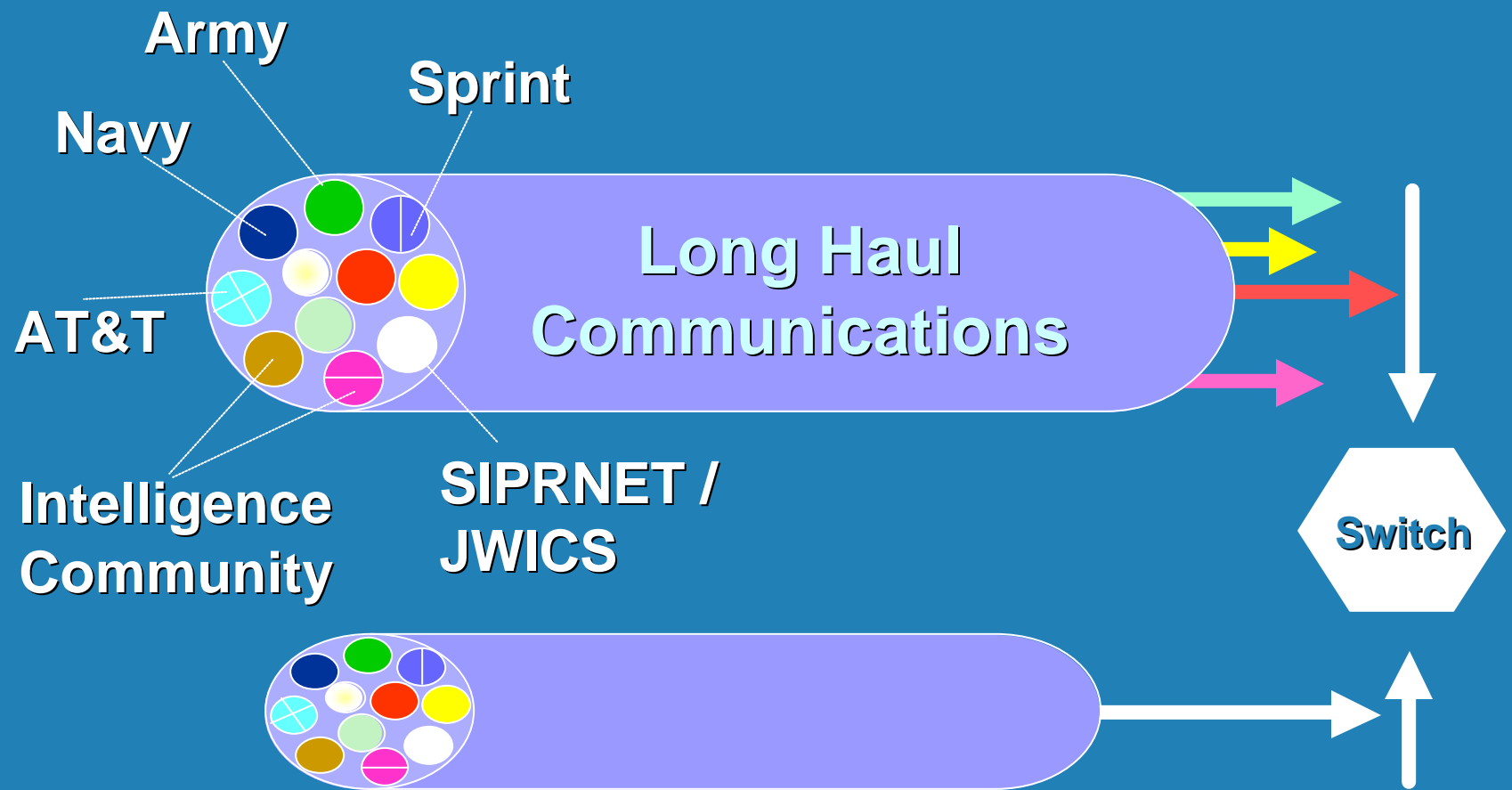
REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 4/22/2002	3. REPORT TYPE AND DATES COVERED Briefing 4/22/2002	
4. TITLE AND SUBTITLE Information Warfare and Cyber Defense			5. FUNDING NUMBERS	
6. AUTHOR(S) Wright, Larry				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)  Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)  Booz Allen Hamilton			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited			12b. DISTRIBUTION CODE  A	
13. ABSTRACT (Maximum 200 Words)  Breifing about information warfare from the Phoenix Challenge 2002 Conference and Warfighter day.				
14. SUBJECT TERMS IATAC Collection, information warfare, information assurance, cyber warfare			15. NUMBER OF PAGES  45	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT  UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE  UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT  UNCLASSIFIED	20. LIMITATION OF ABSTRACT  UNLIMITED	

# USA CIRCA 2002



- Massive networking has made the U.S. the world's most vulnerable target for information attack
- Public and Private infrastructures have become virtually indistinguishable and largely global

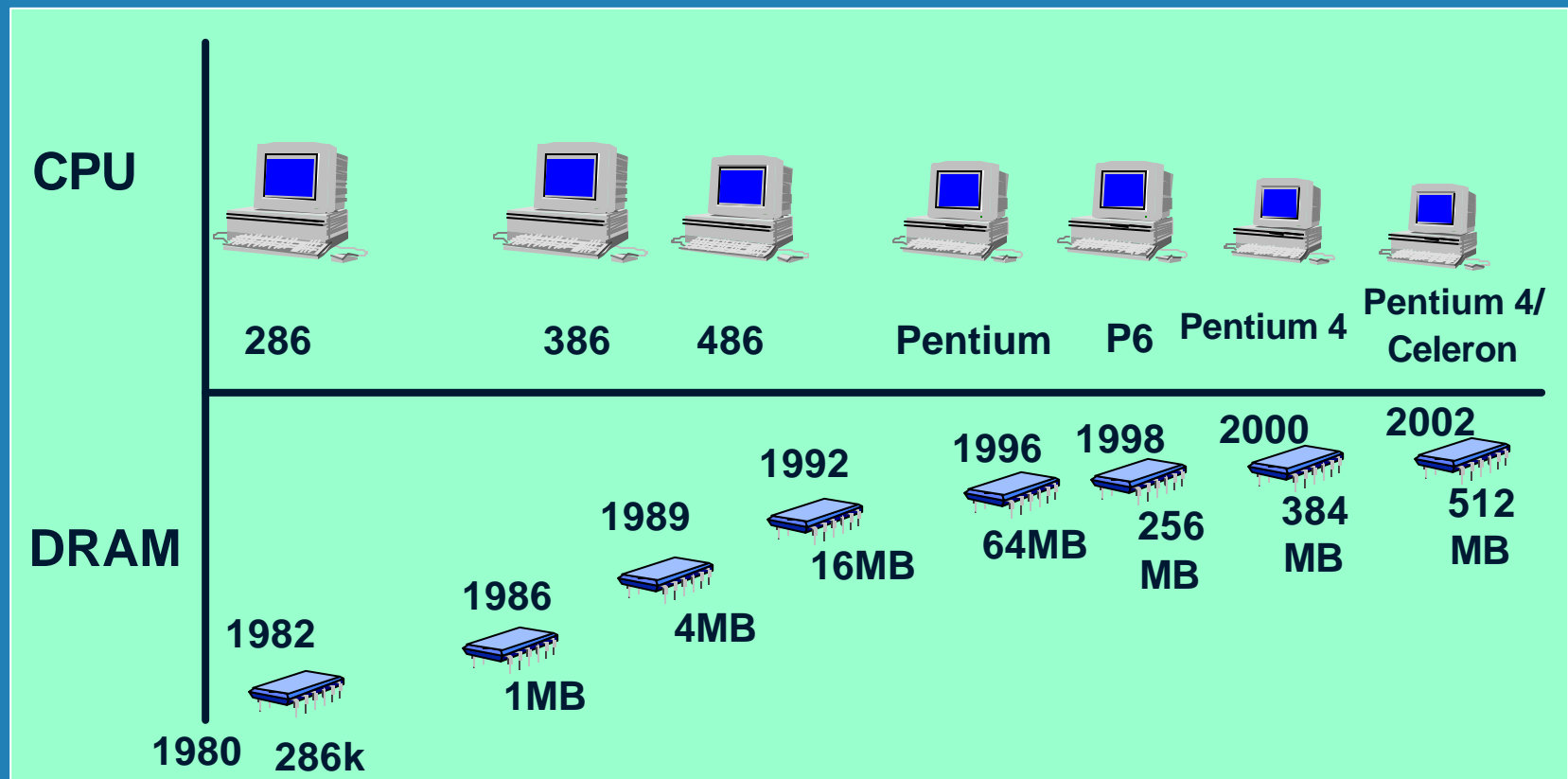
# The Entwined Infrastructure



*USG/DoD is highly dependent on civilian infrastructure,  
and shared capability = shared vulnerability*

# Information Technology Trends

## Power Is Up

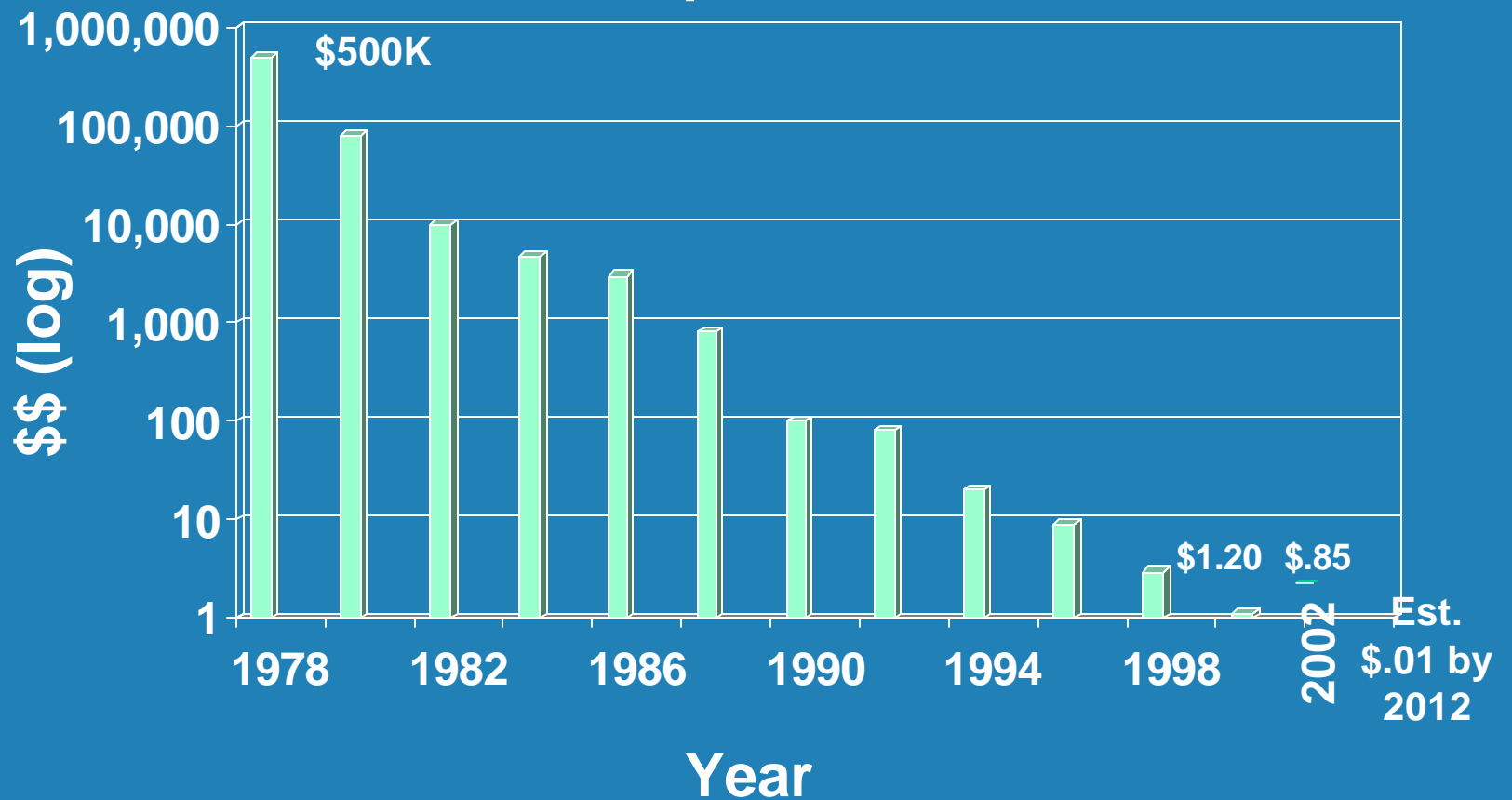


(Source: EIA, CNET, Gartner, Dell -- 2000)

# Information Technology Trends

## Price Is Down

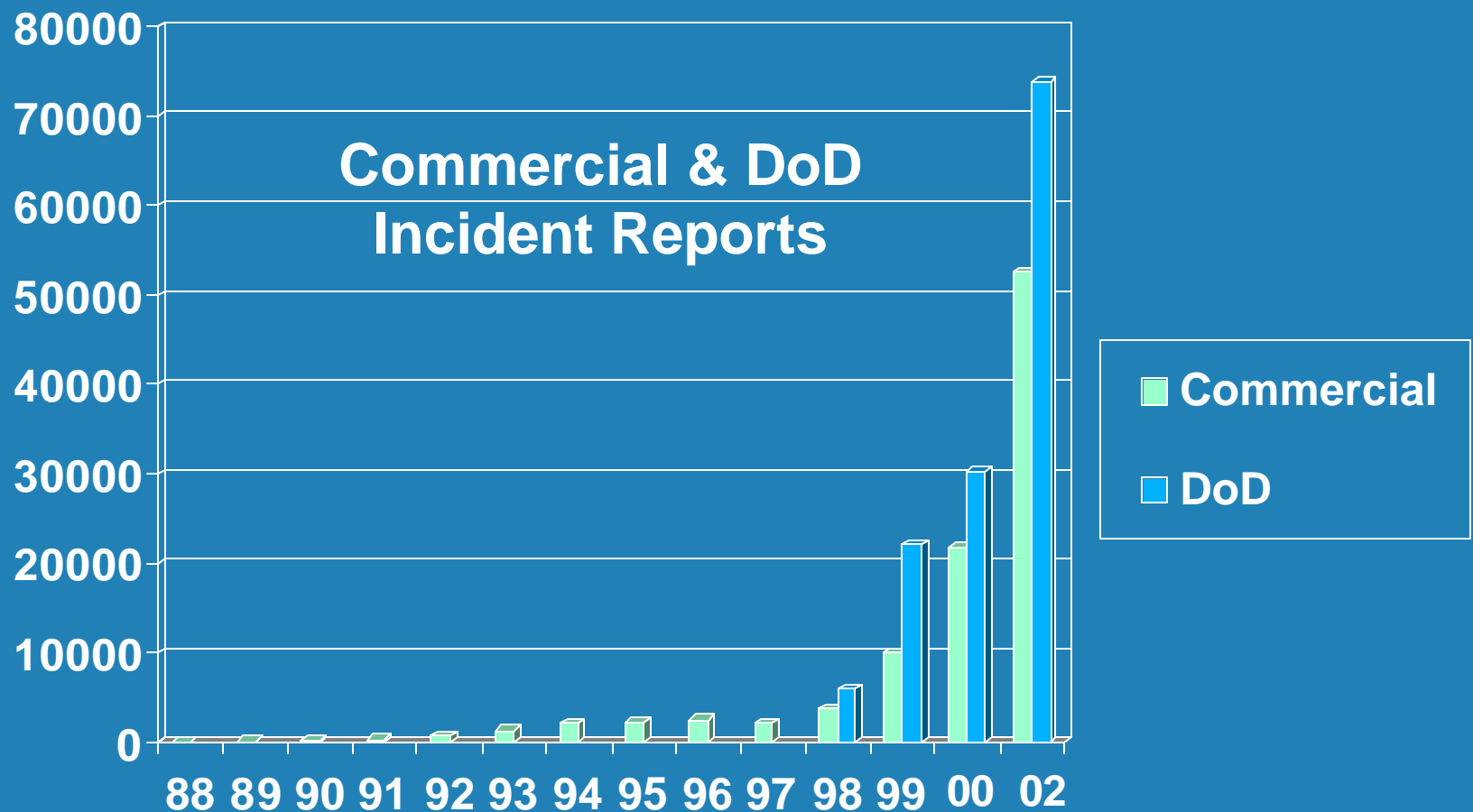
Cost per MIPS\*



\* Millions of Instructions  
Per Second

(Source: Business Week, Jan -- 2002)

# Attacks Are Growing Significantly





# Increasing Vulnerabilities

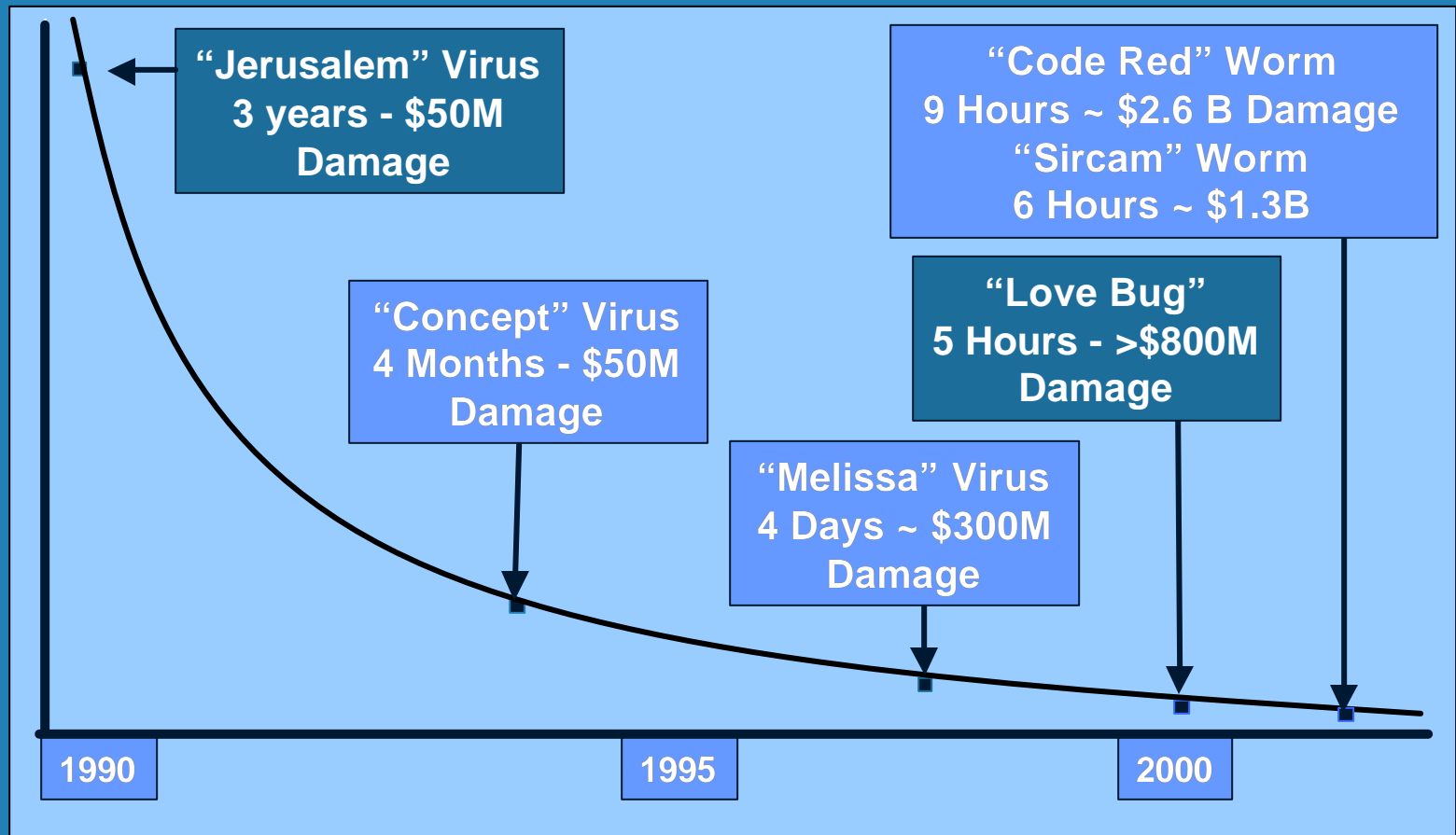
- Number of Intrusions Increasing
- Denial of Service Attacks Increasing
- Velocity and Damage of Viruses Increasing
- Other Nations', Terrorists', and Criminals' sophisticated cyber attack capabilities Increasing

**“...30 computer virtuosos strategically located around the world, with a budget of less than \$10 million, could bring the U.S. to its knees.”**

**-- Center for Strategic and International Studies (CSIS)**

# Virus Attacks: Accelerating in Speed & Damage

Time to Become Most Prevalent Virus



# OMB Report:

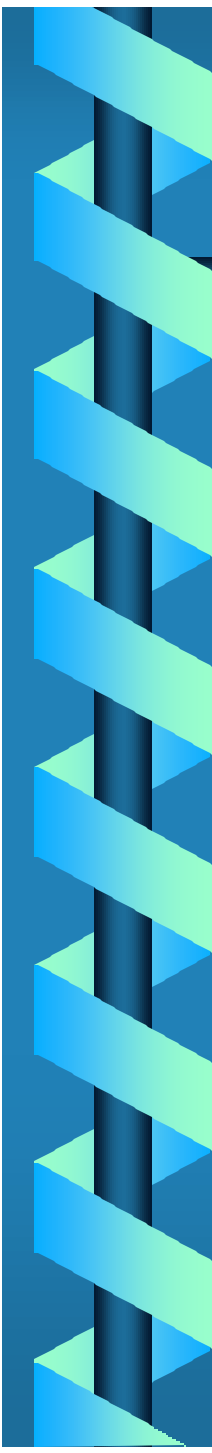
## Most Federal Agencies Unable To Spot Cyber-Attacks

14 Feb '02

### Findings:

- Many agencies have no meaningful system to test or monitor system activity or detect intrusions.
- General lack of policy or programs to detect, report, or share information on vulnerabilities or attacks.
- Most employees lack basic awareness or education on computer security.
- Few agencies ensure contractor compliance on security requirements or background checks.

**In last year's penetration testing, nearly all Federal agencies earned a grade of "D" or lower for computer security – DoD earned the only passing grade.**



# Information Operations

# Information Superiority

LEVELS  
OF  
WAR



Range of Operations

# Information Operations

## Focus Areas

Policy  
Legal  
Organizational  
Operations  
Technology  
Architecture  
Info Assurance

## Responsibilities

NON-DoD  
STATE FBI  
AGENCIES/  
CORPORATIONS

NCA/JOINT  
STAFF  
CINC's

NCA  
CINC's

CINC  
JTF

STATE  
NCA  
CINC's

NON-DoD  
STATE FBI  
AGENCIES/  
CORPORATIONS

Strategic  
Information  
Operations

Operational  
IO

PDD-68

Tactical  
IO

PDD-63

PDD-56

## Elements

- PSYOP
- Deception
- EW
- OPSEC
- Physical Destruction
- CND
- CNA

# Knowledge and Interest Are Widespread

## IA / IO / IW A 10-Day Sample

	E-mail	Links	Articles	Web Sites
IA	38	32	23	2350
IO	22	16	8	2713
IW	7	11	2	26
Related Subjects	16	34		
Conferences	5	5		2

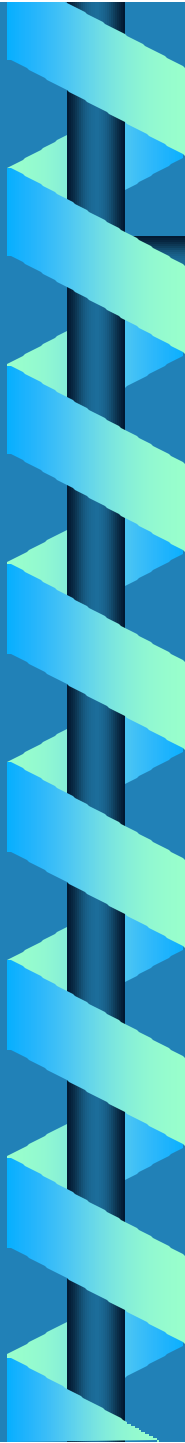
January 2002

# IO “Threat” is Very Non-Traditional

- The IO “Threat” aims to diminish or destroy DoD’s capability to gain and maintain Information Superiority
- Examples include:
  - Trusted insider who takes advantage of access
  - Insertion of malicious code into our system
  - Modification of our hardware or software, including possibly at the supplier level
  - Remote “virtual” attack
  - Empowered “virtual” agents
  - New approaches that have not yet been discovered
- Murphy’s law, natural events, and system fragility all exacerbate likely problems
- Commercial sector will not meet all USG/DoD security needs



# The Insider Threat

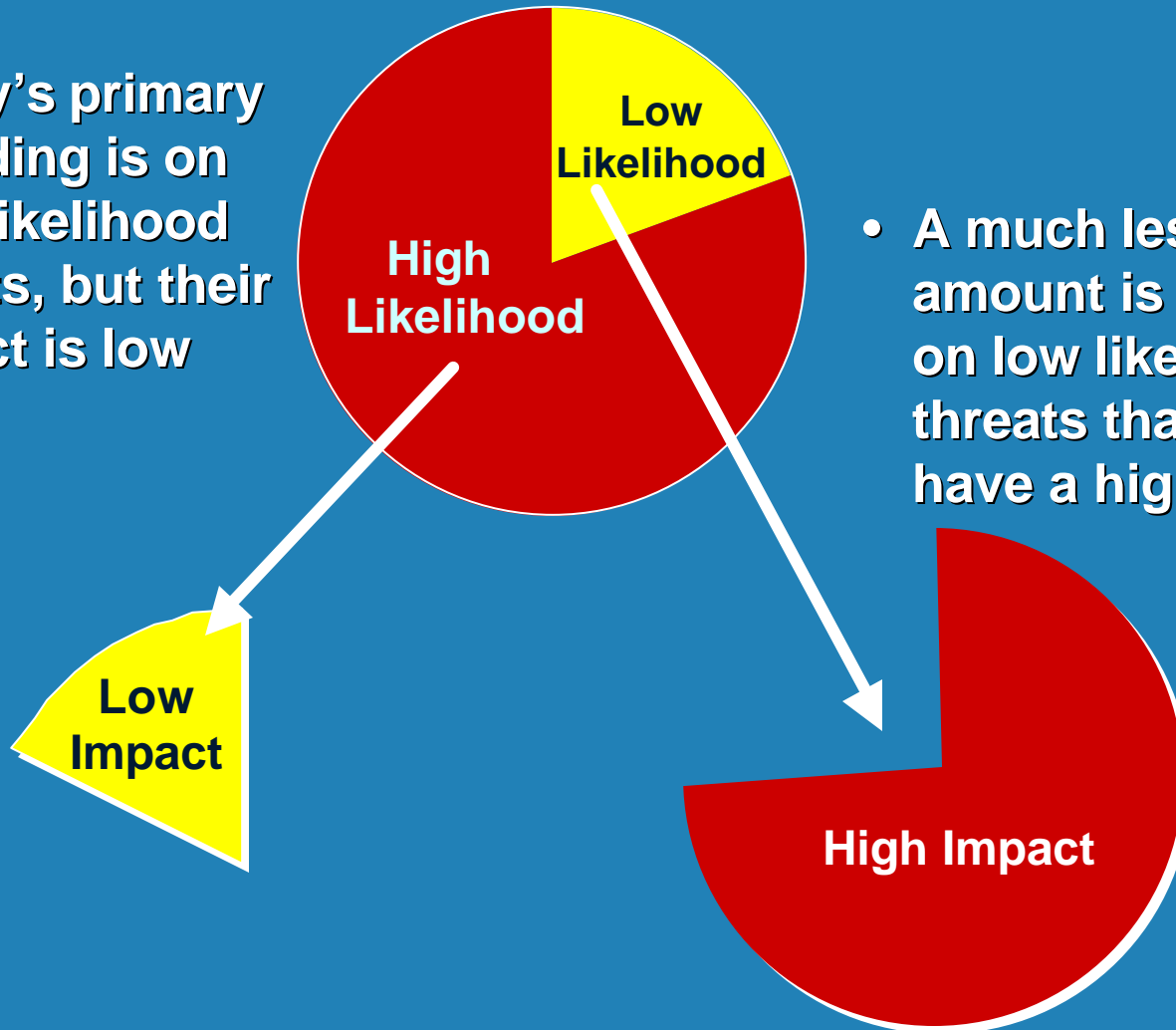


		Internal Process Knowledge	
		High	Low
Technical Literacy	High	<b>Greatest Threat</b>	<b>Demonized But Insignificant</b>
	Low	<b>Significant Threat</b>	<b>Insignificant</b>

Source: GartnerGroup  
Report 5605

# Today's Spending Profile

- Today's primary spending is on high likelihood threats, but their impact is low



- A much lesser amount is spent on low likelihood threats that will have a high impact

# Today...

- Broadly based, fairly uncoordinated USG/DoD efforts are underway
- Public awareness of IW and IA issues at home and abroad is dramatically greater
- Internet use has exploded and USG/DoD use and dependence on the internet has grown exponentially
- We have an increased appreciation of our vulnerabilities from IW
- Remediation and preparations for Y2K diverted focus and potential funds from IA/IW resolution
- A tremendous amount of energy is ongoing nationally, which is likely - over time - to substantially improve U.S. IA/IW capabilities
- A combined WMD/IW attack could be potentially devastating

# World Trade Center: The Real Target?

- The 1993 World Trade Center bombing appeared to be a traditional Terrorist attack -- significant because of its size and planning on U.S. soil
- In fact: The Terrorists intent was to topple the towers on Wall Street inciting a crisis in U.S. financial markets
- Therefore, “intent” to impact/degrade/destroy the U.S. Economy has been demonstrated
- How long until there is a Cyber-terrorism event with the same intent?



# World Trade Center: September 11, 2001

- The 9-11 World Trade Center attack went well beyond a traditional Terrorist attack -- The long term planning and coordination on U.S. soil coupled with the attack on the Pentagon made this an act of war
- In fact: The Terrorists intent was to incite a crisis in U.S. financial markets and demonstrate U.S. inability to protect itself
- Once again, “intent” to impact/degrade/destroy U.S. infrastructure was clearly demonstrated
- How much worse would 9-11 have been if it included a Cyber-terrorism element with the same intent?





---

# **Our National Security Posture**

# National Security's Changing Landscape

- Our concept of national security has always pivoted around the physical and economic well-being of the American people.
- For 200 years, this protection has largely been achieved beyond US shores.
- Today, defense of our economics and people must take place on US soil too!
- Threats may now even be “remote” -- attacks against the US proper, from beyond our shores.
- In the Information Age, our wealth, security, and functionality are all rooted in our ability to control information.
- National security can no longer isolate the role of DoD and the Intelligence Community from the business and private sector.

**Our national security must now become the responsibility of the United States -- Not simply the Defense Department!**

# We Are A Nation At Risk

- Today, in the Information Age, we are the most vulnerable:
  - Each of our infrastructures is dependent on others
  - Globalization and financial integration is pervasive
  - We must protect everywhere from attacks anywhere
- The conflict is engaged: Solar Sunrise, Moonlight Maze, Melissa, Love Bug, Denial of Service, Code Red, Sircam
- The “nuclear threat” now is widely available to almost any nation or group as WMD or Information Warfare technologies
  - Consider information as a weapon of mass effect (WME)
- NSA conducted a significant number of Red Team exercises during the last five years, using tools and techniques downloaded from the Internet
  - 99% of attacks undetected

**We are awaiting a “Cyber Pearl Harbor,”  
when we are already involved in a “Battle of Britain”**



# So What?

- Our concept of national security must adapt to this changing world. In fact, a new concept already is emerging. It encompasses:
  - Traditional concerns
  - National critical infrastructure protection
    - Including critical private infrastructures
  - Concerns that have not been traditional focus of national security: e.g., currency, privacy, intellectual property
  - Protection of foreign networks and systems upon which we depend



U.S. Commission on National Security/21st Century

## The Hart-Rudman Report

31 January 2001

### Road Map for National Security: Imperative for Change

- Serious Gaps Exist in Agencies ability to Protect, Prevent, and Respond to Terrorist Threats
- A “Catastrophic Attack” is likely to strike the U.S. in the next 25 years
- Need to Reorganize the State and Defense Departments and Invest in Education and Scientific Research
- Create an Independent Cabinet-level National Homeland Security Agency to Coordinate a National Strategy against Terrorism (WMD & Cyber)



# 2025 Foundational National Security Elements

- US remains economically strong, retains role in shaping int'l environment
- S&T advancing at exponential pace, widely but unevenly distributed
- World energy, water resources, and global aging become significant factors in the national/global security equations
- e-Commerce transcends national boundaries, global interaction in a multitude of markets on a hourly basis 7/24/365.
- Asymmetries multiply, threatening US response capabilities
- WMDs proliferate to a wider range of state and non-state actors
- Conflict will resort to forms and levels of violence shocking to our sensibilities
- Alliances and coalitions will be increasingly difficult to establish and sustain



# Issues and Observations

# Too Much Data; Too Little Knowledge & Understanding

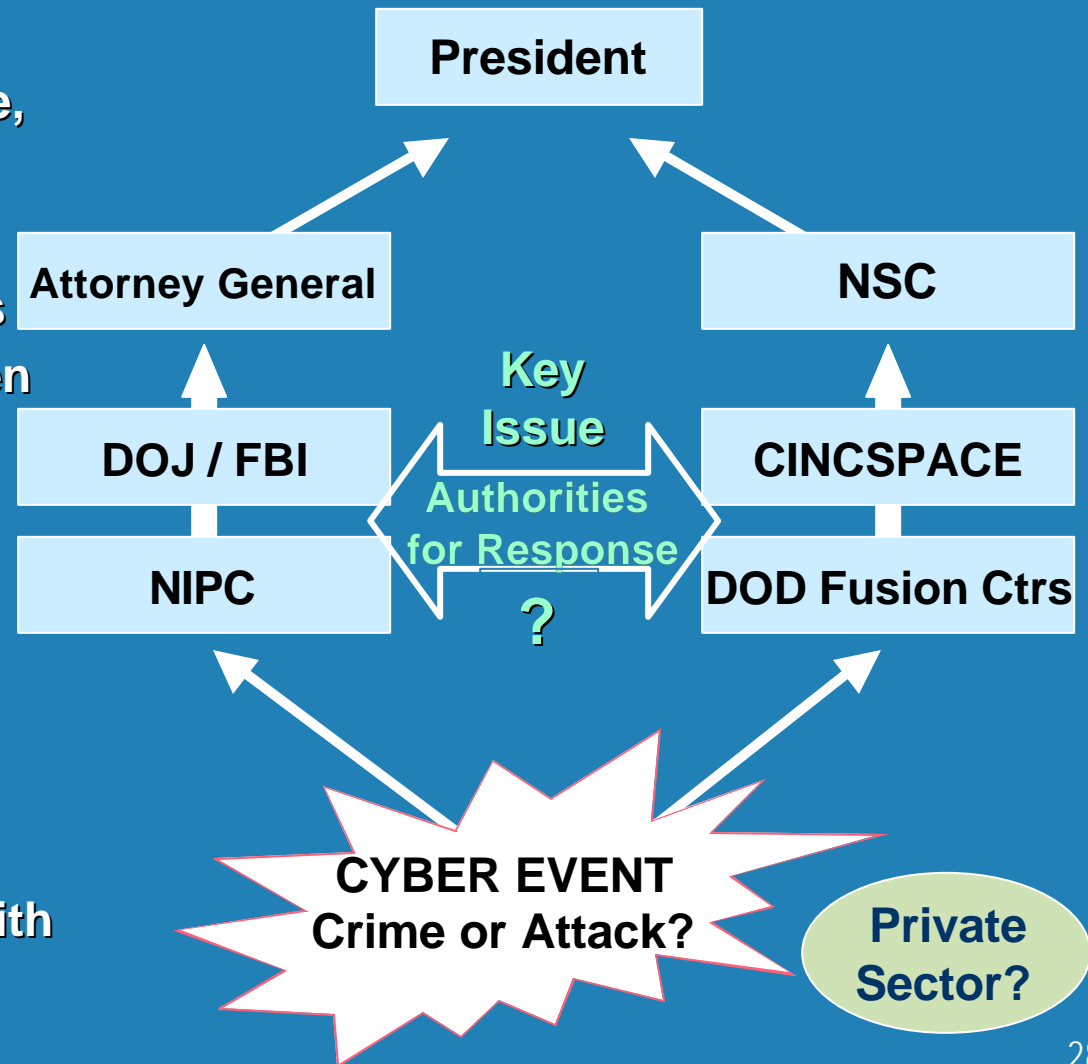
- Information Superiority, like information assurance, is dependent on taking a large volume of data, sifting through it to gain key information, leading to knowledge that can be applied as understanding.
- What We Have:



- Today, the US can gather a vast amount of data through a variety of sources and sensors.
- Some of that data can be sifted to find the nuggets of key information.
- A lesser amount is converted to knowledge, and even less is really understood.

# Issues in Responding to a Potential Cyber Event

- How do we handle an incident when it is not clear whether it is a crime, a foreign attack, or both?
- How should responses be coordinated between National Security and Law Enforcement?
- How should responsibility be handed off once the attacker/criminal is identified?
- How do we interface with the private sector?



# Issues (con't)

- Can a trusted system be composed of untrusted components?
- What role can Active Defense play in Defensive IO?
- Complexity is growing faster than solutions
  - Increased complexity:
    - Makes it more difficult to defend our networked systems
    - AND
    - Makes it more difficult for an adversary to predict and evaluate the effects of his attacks
- Defending against information attack is more critical and more difficult than conducting an information attack against an adversary
- From an operational perspective good security often conflicts with getting things done



# Conclusions



# Current Status of 1996 DSB Recommendations

<u>1996 Recommendation</u>	<u>Pre 9/11 Status</u>	<u>Post 9/11 Status</u>
1. Designate an accountable IW focal point	G	G
2. Organize for IW-D	Y	Y G
3. Increase awareness	Y	G
4. Assess infrastructure dependencies and vulnerabilities	R	R Y
5. Define threat conditions and responses	Y	Y G
6. Assess IW-D readiness	R	R Y
7. "Raise the bar" with high-payoff, low-cost items	Y	Y

# Current Status of 1996 DSB Recommendations

<u>1996 Recommendation</u>	<u>Pre 9/11 Status</u>	<u>Post 9/11 Status</u>
8. Establish and maintain a minimum essential information infrastructure	R	R Y
9. Focus the R&D	Y	Y
10. Staff for success	Y	Y G
11. Resolve the legal issues	R	R
12. Participate fully in critical infrastructure protection	Y	Y
13. Provide the resources	R	Y G

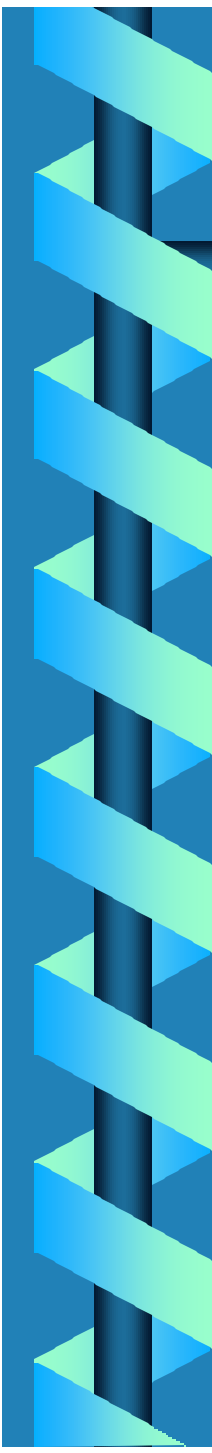
# Who Has Responsibility?

	Cold War	Now
Threat Assessments	IC	DoD / IC / USG Private Sector
Indications & Warning	IC	DoD / IC / USG Private Sector
Attack Characterization & Response	CINCs JCS	DoD / IC / USG Private Sector

**A Shared Responsibility**

# In Some Areas Even 9/11 Did Not Cause Change

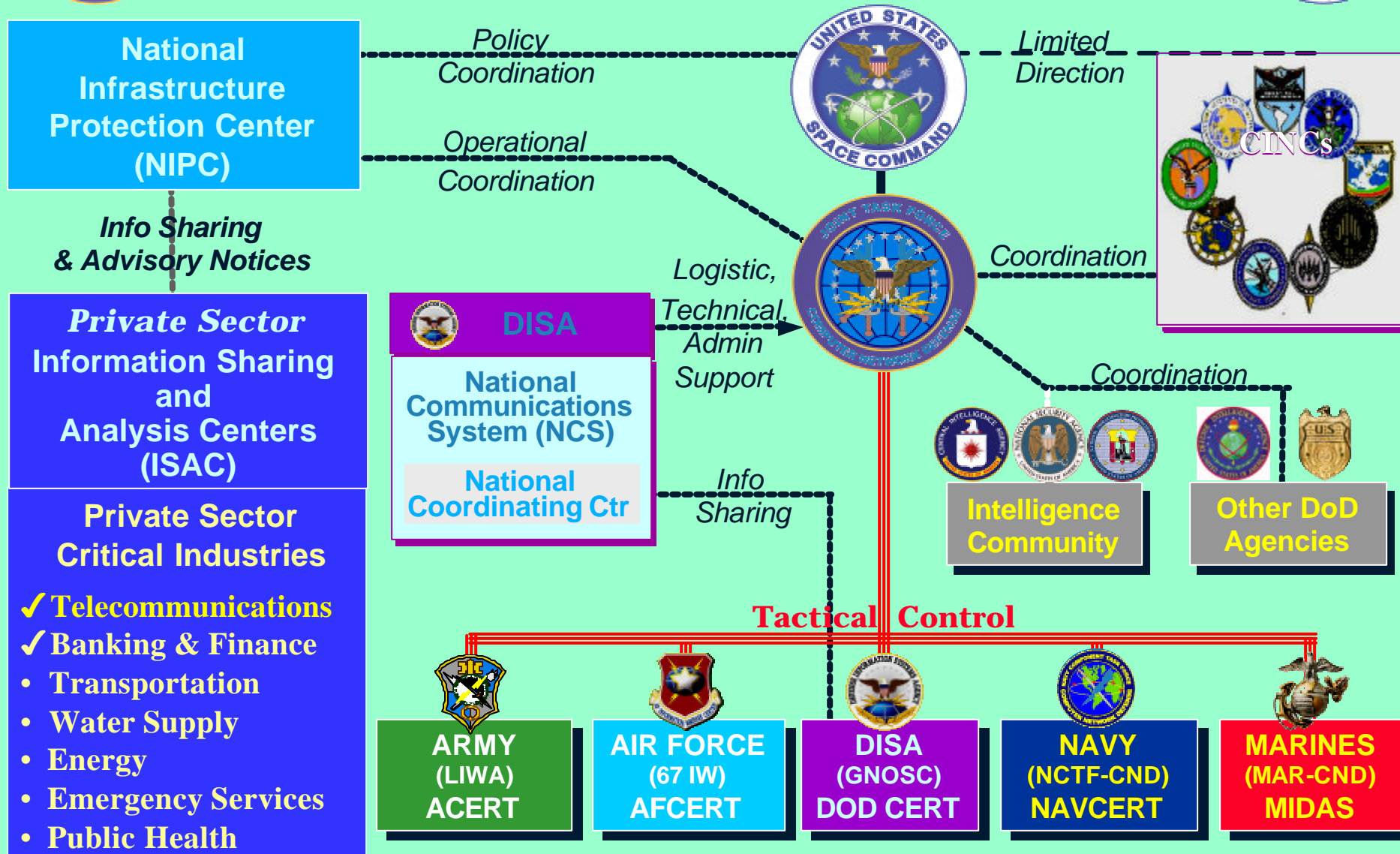
- **FBI Report – April 2002**
  - 90% of businesses and government agencies suffered hacker attacks within the past year.
  - Only 1/3 of those attacks were reported.
  - 80% of those surveyed acknowledged financial losses however, only 44% were willing or able to quantify the damage (~\$455M).
  - 78% admitted employee abuse of Internet.
  - 85% had detected viruses on their networks.
- **Conclusion: “Now, more than ever, the government and private sector need to work together to share information and be more cognitive of computer security...”**



# Back-Up Slides



# CND Relationships



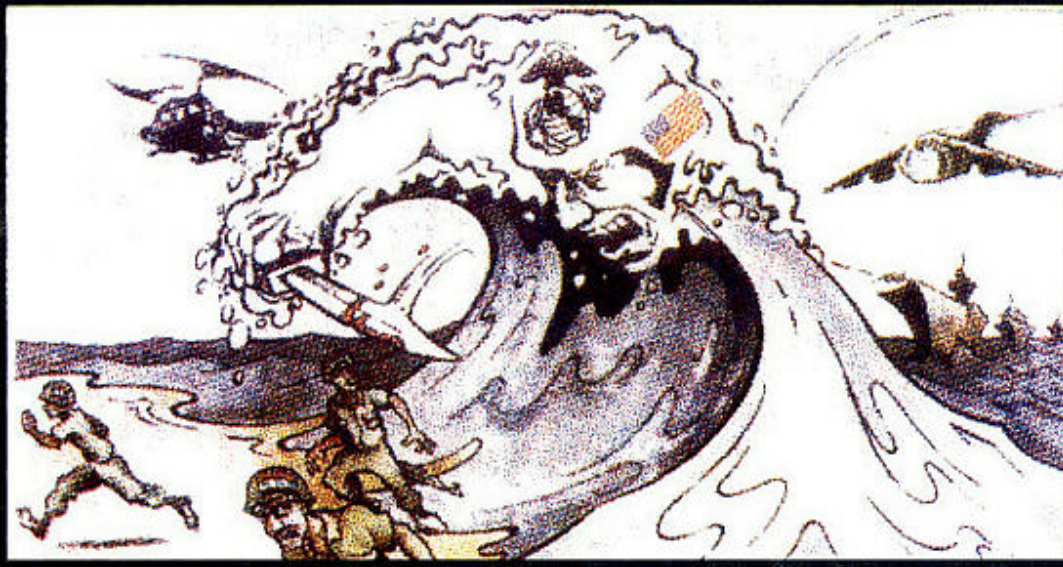


## Elements of IO

# PSYOP

**Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.**

JP 1-02



## Elements of IO

# Deception

Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

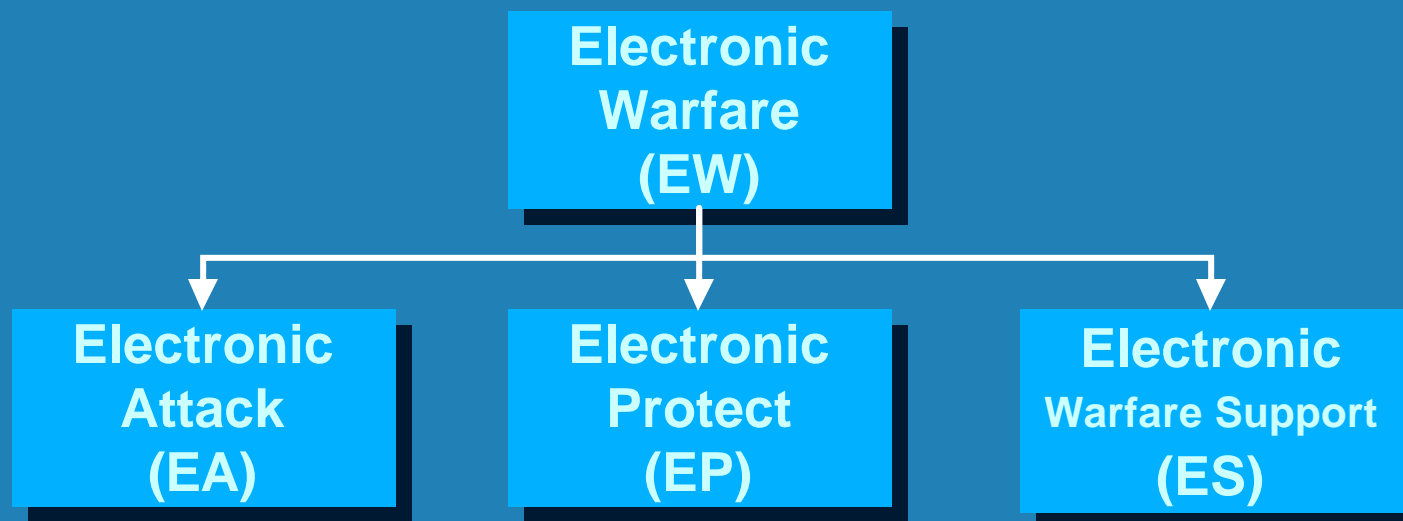
JP 1-02



# Elements of IO

## EW

Electronic Warfare (EW) is any military action involving the use of *electromagnetic* and *directed energy* to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within Electronic Warfare are:

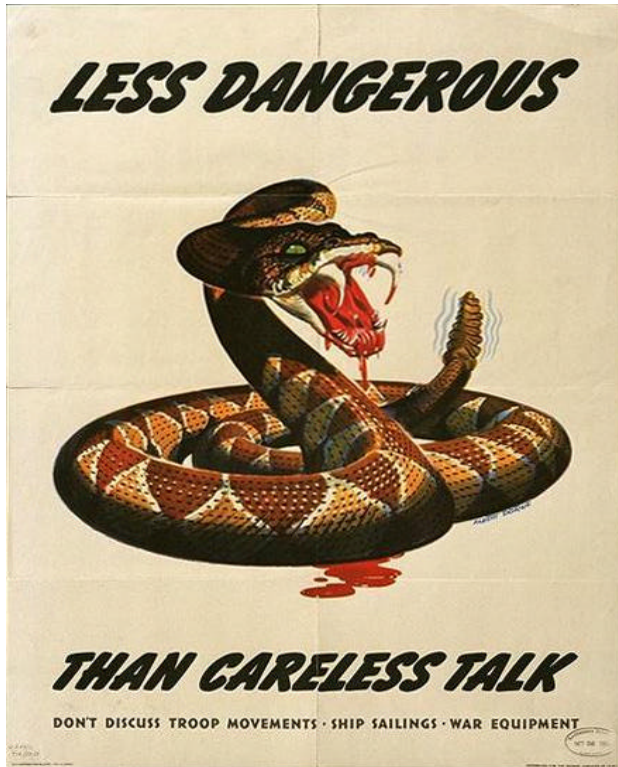


# Elements of IO

## OPSEC

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems
- Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation





## Elements of IO

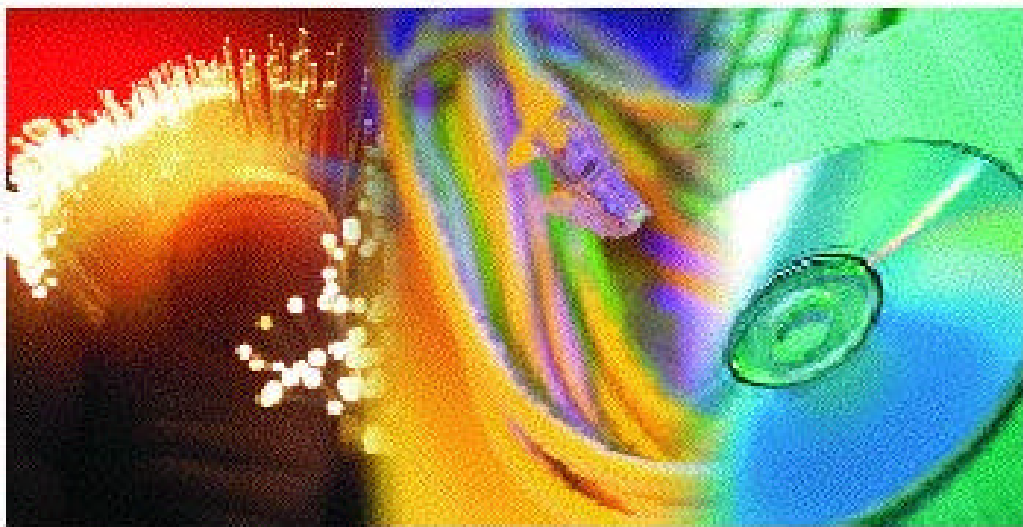
### Physical Destruction

- Physical attack/destruction refers to the use of “hard kill” weapons against designated targets as an element of an integrated IO effort

JP 3-13

- Application of combat power to destroy or neutralize enemy forces and installations.

FM 3-13



## Elements of IO

# Computer Network Operations

**CNO – Computer Network Attack  
Computer Network Defense (CND)  
and Computer Network Exploitation  
(CNE) collectively.**

DCID 7/3

# What Has Changed?

## 1980

- Monolithic Soviet Threat
- Bi-polar World
- Democracy vs. Communism
- Politics Dominate
- Perimeter / Bastion Concepts
- US Vulnerable Abroad
- Pre-PC Environment
- Peak of the Industrial Age

## 2002

- US Dominant Global Power
- European Union
- Global Economy
- Economics Dominate
- US Military Budgets ↓
- US Vulnerable at Home
- Computers / Telcom Pervasive
- Dependent on INTERNET
- Rate of Technology Change ↑
- Dawn of the Information Age

**We Are Redefining “National Security”**

# Information Assurance - Current Status

- Architecture: A solid journey is planned, but the roadmap is incomplete.
- Technology: New developments race ahead of understanding (vulnerabilities, dependencies, reliability) -- complexity is growing faster than results
- People: Limited bench strength.
- R&D: Not using the right seed corn.
- Policy & Legal:
  - Cold War Policy + 19th Century Law ≠ 21st Century Solutions



# The Time is Right to Make Progress in Protecting Our Infrastructures

- 8-10 years of experience and study of these issues
- Congress and the Defense Department are sensitized – Particularly since 9-11
- Foreign awareness and programs show substantial growth
- A change in Administration has taken place
- We should lock in and build on key prior recommendations
- Increased private sector involvement